Privacy & Security Standards Workgroup
Draft Transcript
February 28, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody, and welcome to the Privacy and Security Standards Workgroup. This call will run from 2:00 p.m. to about 3:30 p.m. Eastern Time. It's a Federal Advisory Committee, so there will be opportunity at the end of the call for the public to make comment.

Let me do a quick roll call. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Walter Suarez?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anne Castro?

Anne Castro – BlueCross BlueShield South Carolina – Chief Design Architect
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Steve Findlay? David McCallie? Wes Rishel? Sharon Terry? Chris Vane? Mike Davis?

Mike Davis – Veterans Health Administration – Senior Security Architect
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Moehrke? He had dialed in. Ed Larsen?

Ed Larsen – HITSP
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Kevin Stein? John Blair?

John Blair – Tacanic IPA – President & CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay. I'll turn it over to Dixie.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Judy, David McCallie joined.

Judy Sparrow – Office of the National Coordinator – Executive Director
David. Good. Thank you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Hello, David.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Hello.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Hey all of you, I appreciate you calling in. Today we're going to launch an aggressive effort to develop recommendations on two standards. As you'll recall, at the last Standards Committee Workgroup, at the end of the day John Halamka mentioned that at our next meeting on March 28th, I believe, that the workgroups would be announcing their schedule for developing standards to support stage two meaningful use. In our case, we have a couple of requests already in the bin for standards that have immediate need and although they will be supportive of stage two, their primary drivers really are the Direct Project and the Nationwide Health Information Network. So, we started talking about digital certificates the last time and today I'd like to realign or align that whole conversation with the overall process of interaction between the Standards Committee and this workgroup and with the standards and interoperability framework.

Would you advance the slide, please? Okay. These are what we're going through today. We're going to go through this relationship between our workgroup and the standards and interoperability framework. We're going to review an updated focus in work plan for getting these two sets of recommendations forward. We're going to then dive into the discussion about digital certificate standards or requirements and evaluation criteria for those standards.

I meant to take these two yellow things out, but I hope you can see this. It's not as clear on here as it is in the PowerPoint, but what I've tried to do here is depict the process in a swim lane type of a presentation between the interactions between the Office of the National Coordinator, the S&I framework, the overall Standards Committee and our Privacy and Security Workgroup in particular.

The request for recommendations always will come from the ONC. We don't receive any requests for recommendations directly from the Policy Committee or from anybody else. They'll come down from ONC as we know the two before us now have come down from ONC. The Standards Committee will assign—this is a general process overall—it to a workgroup. I know that this is not the latest. We have a later set of slides that we need to get to you after this. That bottom-line should be any workgroup in the Standards Committee, not the Privacy and Security. There is an updated version. But at any rate, our responsibility is really to investigate the standards that are out there to the extent needed for us to make recommendations on what are the requirements for the standard. We don't make a recommendation on the standard itself. We make a recommendation on what the standard must do; I would say requirements and constraints around the standard. Secondly, we recommend evaluation criteria for the standards.

The test case for this overall process is the Direct Project in which our Standards Committee did do two evaluations of that standard and provided the feedback back to the S&I framework. I'll let you go through this at your leisure, but the basic interaction is that ONC gives us a requirement. We take it and the chair of our Standards Committee assigns it to a workgroup. We then take that and recommend requirements for the standard itself and evaluation criteria for evaluating the standard. We recommend that back to the Standards Committee and there is some interaction, direct interaction, with the standards and interoperability framework before reaching a point where we make our final recommendation.

The next slide finishes this off. The evaluation is done by somebody on the Standards Committee. In most cases, I would imagine the evaluation would be done by the same workgroup that develops the requirements and criteria. As an example of criteria, for the Direct Project the evaluation criteria that we used was that the standard be simple, direct, secure and scalable. So those are kind of the level of criteria we're looking for.

Okay. Would you go to the next slide, please? The next one. Okay. Now I'm going to turn this over to Walter to lead us through the revised schedule and where we are now.

Oh—one more point I wanted to make. Today we're addressing the requirements for enterprise level digital certificates. It's important. We have two standards that we are targeting March 28th to get our recommendations presented to the Standards Committee and both of these are enterprise level, not individual level. There is enterprise level digital certificates, which support NHIN Direct, of course, or the Direct Project. The second one is provider directories, where provider is at the enterprise level, not at the individual level. So I think it is doable for us to develop these requirements and criteria by the next meeting.

Okay, Walter.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. Thank you. Thank you, Dixie. So in this slide what you are seeing is sort of a summary of the two points or phases, as we call it here in the slide, of activity of our workgroup and how they relate to the workgroup ... framework. In this first phase, as we call it, what we will be developing are the requirements and evaluation criteria for the identification and selection of standards, in this case, specifically for the two topics that Dixie mentioned. So we would then pass those along to the S&I framework and the S&I framework will process them, do the work, the S&I framework, to identify the ... and then recommend standards and then bring those back to the Privacy and Security or Security and Privacy Workgroup for us to review.

Then phase two will be that kind of due diligence review once we receive back the recommended standards from the S&I framework. We'll review how the requirements and evaluation criteria were applied to the various candidate standards and the selection made by the S&I framework and recommended to us and make sure that we complete that review of that second phase. So we're concerned in the next four to six weeks I guess with this phase one as it relates to requirements and evaluation criteria for organization-to-organization digital certificates and provider directories. That's what this slide was trying to describe.

The next couple of slides talk about the schedule of activities and then the ... in the process of what we will be doing over, again, the next couple of three or four to six weeks. So we start today and today's focus will be on defining the requirements for digital certificate standards that will support organization-to-organization authentication and define the criteria for the evaluation of digital certificate standards that ... would use. So those are two goals .... With respect to provider directories, we will not have any specific action today. We will just review briefly the recommendations from the Policy Committee on entity level provider directories. We can talk a little more later about that.

That's the goal for today. We would then, on March 9th, meet again and divide the call into two basically. The first part would be the digital certificates where we would be reviewing and finalizing the recommendations on requirements and evaluation criteria to be used by the S&I framework. Then on provider directories, we will dive into the details of the recommendation from the Policy Committee on entity level provider directories and then hear from the Newton Exchange and the Direct Project the need and approaches that they are using for entity level provider directories. Then we will finish up with some discussion about the requirements and challenges and if we get to, to talk about the evaluation criteria, but that's probably as much as we will be doing, able to do in this March 9th call.

Then, obviously, on the third call on there, on the last call to your right, the process. These are sort of our internal processes, I guess, that we would do when we would be sending materials to you all for review before the call, so it's sort of organizing ourselves into sets so that we can put together the material and send it to you for your review before the calls and things like that.

Then after the March 9th, we expect that we would need an additional call to be scheduled the week of March 14th. It's a new call that we would want to schedule. This new call will allow us to focus on the

provider directory, definition of requirements and evaluation criteria for entity level provider directories. So that call will be devoted exclusively to really defining and sort of finalizing the defining, basically, of the requirements and the evaluation criteria.

Then the next slide shows the remaining dates and items to work on, so we have already a March 24th call scheduled. In that call we will be finalizing the recommendations on requirements and evaluation criteria for provider directories, entity level provider directories coming out of the discussion that we had on the call, the new call that we are scheduling on the work of March 14th.

Then the last step here will be to deliver on March 28th to the full Standards Committee the recommendations on requirements and evaluation criteria for both, organization-to-organization digital certificate standards, as well as the recommendations on requirements and evaluation criteria for entity level provider directory standards. So that's our plan for the next basically month really, through the month of March.

Let me stop there and see if there are any questions or comments or issues you want to add to this. Any comments?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, are there any questions? Okay.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
All right. Let's go to the next—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
There seems to be someone on the line with a conversation in the background. If you would remember to mute your phones when you're not speaking? Thank you.

John Moehrke – Interoperability & Security, GE – Principal Engineer
This is John Moehrke. Can you hear me?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Hello, John.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I'm sorry. My phone has been cutting in and out, so I think I missed the call at the beginning. Are we going to be getting further into depth on what the purpose for the digital signatures is going to be, even within the constraints of the organization-to-organization? I mean I understand that constraint. That's a good starting constraint, but I was just wondering if we were going to get further into the purpose constraints as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, we have only what was given us by the S&I Framework people, Arien Malec and Doug Fridsma. We will be and we did have Arien speak on our call about the requirements, you know, what their needs are and how they're used.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Okay. So the purpose of the certificates will be for the purpose of securing the direct exchanges?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Exactly. Right.

John Moehrke – Interoperability & Security, GE – Principal Engineer
So it will not include in the scope the purpose of securing the NHIN Exchange traffic or other—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. It does. At the entity level, it needs to cover both of those.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well that's why I was asking about the constraints on the purpose, the intended use of the certificates.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. Those two purposes are exactly it.

John Moehrke – Interoperability & Security, GE – Principal Engineer
What about e-prescribing?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No. That's at the individual level because a provider needs to sign and all of that. Well, you know that. So it's not really e-prescribing. It's really at the organizational level. I'm sure that down the pike we'll be asked to recommend requirements at the individual level for both of these, quite frankly. But right now, our focus is on the organizational level.

John Moehrke – Interoperability & Security, GE – Principal Engineer
The reason why I bring it up is that often times the purpose embedded in the certificate will have a conflict between the necessary attributes for securing e-mail, i.e., the S/MIME purposes of an S/MIME encryption, an S/MIME signature may conflict with the purpose encoded in a certificate for network transport, i.e., TLS or even IPSEC, CPM. So that's kind of why I was wondering if we were going to fork those different transport level types. It's just maybe food for thought. I didn't know if it was already constrained.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I would say that if we see that as a need, a requirement, then we include that in our requirements.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I think the source of our work really comes also from the recommendation from the Policy Committee, which constrains the focus view on organization-to-organization level provider authentication. So at the end, there's basically those three constraints, if you will; organization-to-organization and then being able to support the Direct Project and be able to support the NHIN Exchange Project. I guess those would be the three primary, high-level requirements, which, incidentally is sort of what we would be getting next, in the next slide, if you move to the next slide on the screen.

We talked about the requirements and evaluation criteria for digital certificates, so starting with the requirement what are the basic business, operating and technical needs that the standard or digital certificate might be able to fulfill really. We provide just one example there; for organization-to-organization authentication, we've been saying there are two requirements really to support the Direct Project, to support the NHIN Exchange Project. Here's where we would be getting into clarification of what are the other requirements that a digital certificate standard will need to fulfill and perhaps even point to some of the things that it is not expected in this particular level to support, like the e-prescribing question, for example.

So this is where we want to begin the discussion about requirements and what are the expectations that we would have on the standard to be adopted for digital certificates. I didn't go to the next slide and then we will come back to the discussion of this, but I just wanted to complete the picture with an evaluation criteria concept. So aside from the requirement that we need to identify and define, we need to identify and define also a series of evaluation criteria. What are the kinds of metrics that should be used to evaluate these standards, evaluate them as some objective way and a measure of what is possible?

So we discussed and talked about and this brings back a lot of memories for those that were back in the hippy days, organizing certainly the criteria into two tiers. A first tier, which would be a set of general, basic criteria that a candidate standard will be required or expected to be able to meet to be considered for the recommendation and then a tier-two level of criteria, which are much more measurable metrics,

assessing specific expectations about a standard. To have met already tier-one criteria will be expected to be able to support in order to pass sort of the test for recommendations.

If we go to the next slide, just a few examples of this tier-one criteria include this concept of being simple, scalable and flexible. We can talk about defining these terms in more detail in what kind of developmental stage the standard is that is being developed or has been completed and in test mode or is a DSTU, a draft standard for trial use, mode or status or whether it's being implemented. And to what extent it's a small scale implementation or whether it's a large scale implementation already in place, so kind of defining what level of stage of development the standard is.

Another set of kind of tier-one criteria could be the degree to which the standard is interoperable, linkable, mappable, portable, those kinds of concepts of supporting interoperability. Is the standard secure, auditable, verifiable, the availability and accessibility of the standard, the cost and the degree to which it is technology neutral. So those are kind of tier-one level of evaluation criteria to be used to assess the standard, the candidate—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think we should add to that last one because it always invariably comes up is broadly adopted; that they shouldn't be new. They should be broadly used and proven in actual use. Okay?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Availability and accessibility sort of covers it, but since it always comes up and the whole Implementation Workgroup, I guess they have developed their criteria and that's one of their strong criteria.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. That's good. Yes. So this would be concept related, sort of tier-one evaluation criteria. Then the next slide covers what we are calling the tier-two criteria. This really comes from the criteria that we used back at HITSP when evaluating the hundreds of standards that we evaluated within each of the various technical committees and working groups and all of that. So these were the five criteria basically and categories of criteria. These used a series of codes, like 0, 1, 2, 3 to grade the degree to which the standard met the five criteria.

Suitability was one that included things like discreet naming, needs of the use case criteria. It's essential these elements are included at the legal and regulatory conformance. So it's a general level of meaning, this type of criteria. Suitability. Compatibility was the other one, compatibility with other standards. The ability to support reuse, prefer standard characteristics, so ... this sort of builds into the comment before, the formally adopted, broadly adopted, the degree to which it's adopted, the degree to which it is accepted. Any barriers or ease of access to it, neutrality in terms of the technical vendor products and the degree to which it's a national or international standard.

Then with respect to code sets, whenever there are code sets involved in, harmonize with other standards, frequency of updates and publications, version control mapping, robustness, deficiency. So these are additional criteria to evaluate those. Then there is data element usage, comprehensive, the degree to which it's compatible with other standards, mappable. How much or what kinds of constraints does it have? Then cost and conformance, basically conformance – there is a conformance clause and the criteria defining conformance in the standard and there are some conformance test methods that exist for the standard. So this was kind of a summary of the type of criteria that was used back in history and that ... really ... really want for our own decision of the type of criteria that we will use and that we will recommend to be used by the S&I framework for evaluating the standards, in this case, the digital certificate standards.

Let me stop there and perhaps we can go back to discussing more about the requirements, getting to the discussion about the requirements and then from there, get into the discussion about evaluation criteria

and try to come up with some consensus around the criteria that should be used to evaluate those standards. Should we go back to the requirement discussion? Maybe if we go back to the slide number nine we can add into the requirements slide some more; I guess I already added a couple of more that include supporting the Direct Project, supporting the NW-HIN or the NHIN Exchange Project. So what are other requirements that people see would need to be listed here?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
For starters, I think we all agree that it needs to be X.509 compliant. We've talked about that in the past. That's kind of the taking off point.

M
One of the points that has come up in the past is the availability and how the certificates are distributed and how difficult or easy it is for the entity or organizations to acquire and maintain.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. That sort of spans both of these standards that we're looking at, both the digital certificates, as well as the provider directory, because they see the provider directories as the way not to distribute them, but to at least discover them.

Another topic that's come up that I'd be interested in hearing your thoughts; and this just came up in a separate e-mail conversation is should we require that anything of the certificate authorities that actually, to address your point, that actually distribute these certificates. Should we require that there be any constraints on who you need to use as your CA if you're going to participate in Direct or the Nationwide Health Information Network. I'm not sure how they're pronouncing that these days?

(Overlapping voices)

Mike Davis – Veterans Health Administration – Senior Security Architect
Dixie, there's likely to be restrictions on some providers from various reasons, either they're a federal agency or maybe a state that would restrict the kinds of certificates that they may accept. It may not be uniform across all jurisdictions, however.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. I think to kind of extend upon that, I think at the HIT standards we should be recognizing standards that can be used in those restricted policy spaces. I mean we shouldn't be specifying standards that can't be used in those more restricted policy spaces, but I think, Dixie, getting to your question, I think that is a legitimate thing for the Policy Committee to declare, but I don't think we in the Standards Committee, should be constraining the policies. But we certainly have to be cognizant of what those constraints may be.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. That's a very good point. That's not a standards thing. It really is a policy thing.

M
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's really important, because as we're trying to build this whole Nationwide Health Information Network people won't trust other organizations unless they feel that they got their certificates from some legitimate source.

M
Maybe we need some guidance on this point up front, because it would be, to John's point, we don't want to knowingly maybe exclude a whole class of people because of what we know as policy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, or at least we need to be aware of when we are potentially causing more pain to one group because of a particular decision.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Doesn't some of this come down to level of assurance and all of the hundreds of pages of categorization and description of the various levels of assurance? Wouldn't that give you the flexibility? I mean if a policy says a level of assurance needs to be two then you may have more freedom to choose how you handle your certificate authority than if they say it's level six or something like that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right. Yes. Levels of assurance is clearly a policy space. There is nothing at the certificate level that is constraining any high or low level of assurance, but policy would certainly be one of the policy decisions would be a floor or a ceiling on level of assurance. That would be one way of specifying a policy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I meant with respect to the notion of what kind of certificate authorities would be tolerated. That may be a function of level of assurance that you seek rather than an independent, abstract criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
From a standards perspective the certificates have a field for the certificate authority, but there's no real way and there's no real model for how much that particular certificate authority is trusted or not.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. That's usually encoded in the certificate authority's trust relationship. So you wouldn't be accepting as a legitimate certificate authority root someone, who is not issuing certificates at an acceptable level of assurance. So that would be a way to execute on a policy. If a policy says this particular root we know issues certificates only at level of assurance three; therefore, we can accept that as a legitimate root; whereas, this other one we know has a lot more relaxed rules, so let's not accept that as a trusted root. That's the core of—David, you'll recall this back when we were doing the NHIN Direct stuff. We were saying it really comes down to you have to start with an empty trustor and you only insert into your trustors those that you have a good reason to trust. Which is the opposite model of the current Web browser environment, where the Web browser vendor has prefilled the trustor with a huge number of certificate authorities of all various levels of assurance, including some which are zero level of assurance, so I think that's a good policy statement; that you start with trusting no one.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. John, you captured the spirit of what I was trying to say. That's good. Thank you.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So do we go back? I guess we go back to the Policy Committee and say we're specifying our requirements for the certificate such that they can include the trust, the assurance level of the certificate, but the industry needs a policy with respect to the lowest level of trust of assurance acceptable. Is that right?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes. I think that is the outcome of all of the discussion; that there is some recommendation back to the Policy Committee. I think the Policy Committee would appreciate it if I'm correct. Dixie, these will probably come back to the Security and Privacy Tiger Team that the Standards Committee explain or describe the context of this need for policy of minimal level of assurance so that they can take on that and make their policy decision, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. I can get that back to them. So let's assume there is a floor, a minimum level of assurance for the certificate authority. What do we need? Are there requirements then that we need to put to the S&I framework to capture that? What are they? I mean to me the requirement is that the certificate be able to convey not only the name of a certificate authority that issue it, but also the assurance level of that certificate authority.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, maybe another way of looking at it is you've identified this has to be able to support both, Direct and Exchange—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Those two things are, to me, significantly different in their models and how they're doing things. So are we having one specification that satisfies both or are we intentionally having a specification that would be suitable for one, but not the other?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think this is the same point that John brought up earlier. I think we need a core set of requirements that would apply to both of them and where we see there would be differences we should also specify those differences.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. There certainly will be some differences. I think I like how you came through with that, Dixie, in that we'll probably have a core set, which are common and then we'll have the set while, if you're using the Direct Project transport, you'll have these additional requirements. If you're doing an Exchange style, you'll have another set. Because I think there is a small set of differences, but they're critical differences.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'm unclear what our duty is with respect to how you operate with these certificates versus the standard for the certificate itself. It would seem to me that Direct and Exchange are both using the same standard, but they have different operating assumptions around how you implement the use of the certificate. Is that in our purview to—?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, it depends on how deep we go in defining the standard. If we just simply say it's an X.509 digital certificate that must chain to a trusted authority where the trusted authorities are completely managed by the organization per policy and we stop there then we probably can get away with not having any more differentiation. But if we start saying that the certificate must include a level of assurance attribute then we have to explain what level of assurance attribute we're inserting; what standard it came from; how does it related to the use when the transport is S/MIME; how does it relate when the use is transport of TLS. As we start getting more and more specific we will get more and more differentiated between the S/MIME transports versus TLS transports.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think, again, it seems to me that's not a change in the standard. That's a change in one case in policy, specifying which level of assurance, which could be different for the two use cases and in terms of operational—well, I don't know what to call it—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, undoubtedly, if we specify certain data fields that are required let's say, there is an implication there that an implementation is going to check the CA, the root CA and validate that the certificate is up to date and that kind of thing. But that's not our role. Our role is to specify the requirements for the standard itself.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So maybe my question is really around who specifies the implementation profile; I think maybe that's the right term; because that seems to me what's actually different between those two use cases.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Yes, that's really an implementation guide.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'm not sure what we have to do is what I'm getting at.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I mean I'm not sure what our contribution to this is.

M
Yes. I—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, we need to specify what are some of the required data fields, but I don't think that we specify an application must always check—for example, I don't think we specify that an application must always check whether the digital certificate is still current or whether its date is still current. But we require that the certificate itself say the expiration date or something like that.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Most of the standards in this area have mandatory fields for the certificate. Then they have extensions that you can put on there if you want to, but the point of kind of focusing this because you could argue, let's say, from a risk point of view that NHIN Direct is less risky than Exchange. Because it handles on a per-exchange basis probably only a single record of a single, as opposed to Exchange and that would be handling, potentially multiple. I don't know. You could make a kind of argument like that. So this purpose of the use and the context of the use becomes somewhat significant.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That should be defined by the Direct and the Exchange Project itself. So if the standard for these, the standards that are selected and identified through these criteria are able to be supported by different profiles then the Direct Project would define this kind of "implementation profile" that David was mentioning and describe how the standard is being used to fulfill that requirement. Then the NW-HIN or NW-HIN Exchange Project will develop its own implementation profile as well. That's where maybe the distinction between the two is, but both of them are using at the end of the day the same core, basic standard, right?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. So let me kind of tie together, at least in my mind, what I'm hearing between what David's saying and what Dixie said earlier that I think was a key here. I would feel very comfortable with us concluding this meeting by saying, "Yes, we have selected X.509 certificates." We don't need to go any deeper, but oh, by the way—this gets to Dixie's point—HIT Policy Committee, we've looked at the policy space that you've been discussing, level of assurance, trust building, revocation handling and be assured that the standard we have selected can support the policies that you are looking to decide. Once you decide those policies we recommend that there are some implementation guides that bind the policy decisions with the standards that we've selected here, being just simply X.509 and yes, we don't have that much to do because it's a very mature space.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. John, as usual, you said it better than I said it. That's what I meant—is that it is a mature space and there's—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It's pretty well worked out what the various aspects of doing this are. The detailed, technical spec is solid and well accepted and proven—

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right. I think communicating that to the Policy Committee, I think, is a very useful purpose because often times the Policy Committee will sit and wonder, you know, are we in a mature space? Are we in an immature space? Without the Standards Committee to say, "Yes, we've got your back," they can end up spinning and not progressing.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. So we convey to them that this is a mature standard, but that we need a policy decision on the level of assurance of the issuer the issuer must provide.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The other point, where clarification from this technical standard side back to policy might help is not only certifying that the standard itself is an appropriate and mature standard, but some of the detailed questions that came up in the Direct conversations got pretty confusing. The lack of education on the part of the people participating in the discussion, myself included, but it certainly wouldn't hurt to clarify some of those technical questions so that, for example, interoperability with a federal bridge, what does that actually mean and what does it cost.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Is that itself part of the standard or is that an add-on? There are some other clarifications, which, having said on the policy side, some of these debates are just mystifying to the policy guys.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, considering that some of the largest provider and payer organizations in the nation are federal, on the federal bridge, I think that that is a requirement.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I think in the Direct conversation when we discussed that the issues that came up were cost and complexity. Is that too complicated/expensive/cumbersome to allow the small practice docs to participate in the network? I don't know what the answer to that question was, but that's what got debated.

M
Well, and to be specific—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Really, they'll need to exchange with, for example, the VA.

M
Yes, but to be specific, I mean in the Direct project we were dealing with very small doctor's offices, who were dealing with their local hospital. That small doc office may never, ever need to communicate with a federal partner.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I can't even imagine that. So they're never going to bill Medicare?

M
Not electronically.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And they're never going to exchange with the VA? I don't buy that. I think every provider needs to exchange information with Medicare and with the VA as well and many of them with the military health system as well, but especially the VA and the CMS.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. I mean at some point – we have endless debates on this and Direct also – it comes down to what does it mean to participate in the Direct network if you can't interchange with certain parties. But we've defined a model that allows for various levels of trust, so by definition it's not homogenous unless we insisted on that as a policy thing. So it's a conundrum that we kept stubbing our toe on and I think practice will probably prove out which is the right way to go.

But back to the question, back to sort of what can we be good at or what can we be useful: It may help maybe to clarify some of these highly technical questions so that policy can be set, being aware of what the technical choice is. In other words, you policy setters can require federal bridge connections, but here's what that means and here's what it will cost, in a technical sense what it would cost, the extra complexity. It's almost more of an evangelist role or something for the technology than it is specifying the technology because in this case the technology is already specified.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't even think that that's a policy. I think that that's just a statement of fact; that they have to be able to exchange with federal entities.

Mike Davis, you're on the phone. You're with the VA. If we required that the standards enable interoperability with a federal bridge what would that mean? Would that be do you guys exchange information with small providers? How do you do that?

Mike Davis – Veterans Health Administration – Senior Security Architect
We have fax machines—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Highly secure fax machines.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Mike Davis – Veterans Health Administration – Senior Security Architect
But I'm following the VA is going forward with the intention of communicating with small providers. Our pilots with NHIN Direct is clearly in that direction. I agree with you. It would be, from our perspective, disastrous to have a system that we could not use to exchange with providers. It's quite fine that the VA and DoD can communicate together, but it's not fine that we can't communicate with others.

I think we have to take the view that the federal people have to comply with FICAM and we should also be looking at at least the draft national strategy for trusted identities in cyberspace, which specify FICAM. It's the national strategy seems to be heading in this direction. We should be aware of those things at least.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. I also know that there are a number of HIEs out there that the ability to exchange information between the VA and private sector is one of their key selling points, so I know that there is a need. Well, you've just said that there is a need for those exchanges to happen.

Mike Davis – Veterans Health Administration – Senior Security Architect
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
For example, I think it was last week Microsoft HealthVault indicated that all HealthVault subscribers can use NHIN Direct. So the digital certificate that HealthVault gave to me on Sunday when I went into my HealthVault is a federal partner authorized certificate. I can communicate. So this is kind of the unintended things that we need to watch for is the Direct Project is enabling patients themselves to participate in directed communications. Is a patient communicating going to be prohibited because of FICAM? I can't talk to my own personal healthcare provider because of FICAM, even though neither one of us are doing federal communications?

John Moehrke – Interoperability & Security, GE – Principal Engineer
No. I'll get back to the fact that the discussion we're having has nothing to do with the standards being selected. The standards, whether they be the certificates issued by HealthVault are identical. It's the trustor that's different and the procedures and the policies behind that trustor. So we've enabled the HIT Policy Committee to make those decisions, but I want to be very careful on instructing them that they should just go ahead and make sure all directed exchanges are using certificates that are cross certified, certified ....

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Again, I think what will cause people to stub their toe is that they don't know what that tradeoff entails. I mean the simple answer is, "Sure. Why not require that?" If the answer comes back it's $10,000 a seat or just make up a number. They say, "Okay. No, that's not a good idea." Somebody needs to educate on what these choices mean from a technical point of view.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
It's not $10,000 a seat.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No. I know. I just made that number up, but the point was there were some people in our conversation in Direct who thought it was potentially prohibitive. Most of us didn't know what that meant, but that's what I'm suggesting—we could make sure that's not a mystery—that that's actually something well understood.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think that the framework for patients ... I don't think we're trying just to provide ... for patients to communicate with that are a PKI level.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No, but Direct will definitely be.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes, that is in the context of Direct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I can't even imagine that we would come up with certificates that couldn't be exchanged with the federal government. I mean there's just too high of a percentage of health exchanges that are with federal entities, a large percentage of them. So if we came up with a certificate that couldn't be used with the federal government I think that that's pretty short sighted and not recognizing reality.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, getting back to this is the HIT Standards Committee and I think we're selecting X.509 certificates there's nothing forbidden about whether those are individually issued, i.e., self-signed versus federal PKI. It's policy binding that we're enabling and it's the policy that would potentially prohibit. Now we're having this policy discussion.

M
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So the only thing that's really needed to exchange information with a federal entity is the cross trust relationship? Are there fields in the certificate that FICAM requires that we need too or do we just say that it must be compliant with FICAM? What do we do? Mike, I think that you're the best one to answer that. Are you there? Are you on mute?

Mike Davis – Veterans Health Administration – Senior Security Architect
I am on mute.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Good. I'm glad you're there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Dixie, before Mike goes into his answer, I unfortunately have to sign off. Unfortunately, when the call gets really interesting, so I will just catch up with you later and find out. I apologize. Mike, go ahead.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Thank you, David.

Mike Davis – Veterans Health Administration – Senior Security Architect
This is great. John's point that we just specify a technical standard for PKI and irregardless, it fits whatever the policy is; that's why I think we should go back to the Policy Committee and maybe get some guidance, but I don't think there's anything. There's nothing special in the certificates themselves except they're signed by someone who is a participant in the bridge and you know who they are. You can validate that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. So as far as ... in the certificate it's nothing special. It really has to do with the trust relationships.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
The question I have is really if we are focusing on organization-to-organization when we think of the Direct Project and the involvement of, say, its patients and enabling a patient to communicate directly to his or her provider that seems to get into the individual level kind of exchange that we're trying to avoid, right?

Mike Davis – Veterans Health Administration – Senior Security Architect
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
A lot of the Direct exchanges, it's recognized a lot of them will be individual-to-individual, but there are still perceived as and considered organization-to-organization.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Well, I think this is one of the things we discussed, in fact, earlier this morning on the individual level provider directories; that in reality even in the Direct Project most of exchanges are organization-to-organization. It's just they're direct between organizations, but they're not really. By virtue of saying direct it doesn't mean individuals. It means more the direct exchange between organizations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's why I wanted to bring up that point; because I think still they specify the technical standard for each certificate and PKI that that will fill the direct exchange, the Direct model basically, but the organization-to-organization will still fulfill our requirement. The question is whether or how would Direct, the Direct Project, take that into the next level, which is now we need to go to an individual, particularly a patient sending a document to a provider.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. That's totally out of scope of this conversation. I mean this is organization-to-organization. John, at the beginning of our conversation you said that when you asked about would we be getting into more depth of a purpose regarding Direct versus the Nationwide Health Information Exchange, what differences would you see in the requirements for the certificates between those two?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, it's primarily within the X.509 certificate are attributes that are scoping what the certificate can be used for, i.e., it says this certificate can be used for S/MIME encryption. This certificate can be used for S/MIME signature. This certificate can be used for TLS. So the things that the certificate is authorized or not authorized really to do, but is intended to be used for is part of what's encoded in the certificate.

Now, getting back to what we were doing, I don't think we here need to define that. I would prefer to keep it as high as we can and say look, we've enabled you, Policy Committee, to have organizational trusts. We've allowed you to be able to bind that to a level of assurance. We've enabled you to have specific purposes, such as S/MIME encryption and S/MIME signature, long-term signature, long-term encryption. So I think if we were to basically indicate the things that we are enabling that would be very useful to the Policy Committee. But by us saying these certificates at the HIT Standards Committee definition must have the purpose of use nailed down to nothing other than S/MIME encryption and S/MIME signature we will then be creating an HIT Standards definition that can't be used for TLS.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. So it sounds to me like we're back to the point where we want them to use X.509 certificates and I hear two things we want to send back to the Policy Committee. One is the need for a floor level of assurance and the other is whether we need to enable exchange with federal health entities. In posing those two questions to the Policy Committee, we need to tell them what these certificates enable them to do.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. I would say it slightly differently in that we're actually not asking them a question. We're saying that we have selected a standard, X.509 that enables them to make the decision what level of assurance they want to nail it down to, what trust relationships they want to nail it down to, what age of certificate, what size is key, what purpose of uses. We've enabled you to make those selections and it would be up to the Direct Project, per se, to take the combination of the X.509 declaration from us, the policy from the Policy Committee and say, "Inside of Direct that means this," which I hope is the same thing that they've already said. So we're not really saying please tell us this so that we can do something more. I think that something more should be done by the Direct Project for the NHIN Exchange Project or the S&I framework project.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I sort of agree with that. I think the only thing that I would add is that in communicating back to the Policy Committee that they are now enabled to make these policy decisions. I think we need to describe the kinds of policy decisions we believe they need to make and give them that kind of a frame of reference.

Otherwise, again, for the most part Policy Committee members are policy level people, so I don't know that they necessarily would understand what are the kinds of options, policy options and policy level determinations that they need to make. So in communicating—

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes. For example, the question around level of assurance or support for federal, what does that mean to the Policy Committee? Well, it means that the certificates must chain to the certificates issued in an operational environment, must chain to a certificate authority, which is cross certified with the federal PKI bridge. So they understand that if they make that choice it means that this now is declared as an operational requirement.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that's a legitimate thing for us to take back to the Policy Committee. I think that I've heard two requirements from this conversation; one was kind of an assumption at the beginning. One is the X.509 certificates and the other is the ability to support both, direct exchanges, as well as NHIN exchanges. Right?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. The level of assurance in the certificate is among the mandatory fields. Is that right?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Actually, how level of assurance is practically implemented today is through the trust authorities, what branch the certificate goes to. For example, VeriSign has a whole boatload of different certificate branches and whichever branch your certificate goes to will indicate what level assurance that certificate was issued at. The same is true about all of the other certificate authorities. So the level of assurance is defined by the root certificate that signs the end certificate that you're using. So there's not really an encoded attribute, although there can be. But the actual trust relationship is purely done by the certificate issuance.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. So it's really just they captured a certificate that's already in. Of course, that's a mandatory field.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But I heard also and, John, you pointed to those, three things. We heard the three requirements that, Dixie, you pointed to; X.509 and support of Direct and ... exchange. But I also heard three areas where we would want or we should let the Policy Committee make a decision. One is the level of assurance. The other one is purpose of use. The other one is cross certification with a federal bridge.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I've already captured that. That's a separate topic. I already captured that as well.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
But I wanted to ask, John, if there are any others that you think are important for the Policy Committee to be aware of.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, I mean the other one is the one that David and I were talking about; what's the ramifications of not requiring federal? What does that mean from a technology perspective? Well, it means that you have other trusted roots that you are directly trusting. You're not relying on the federal bridge to tell you to trust them. You're saying, "Yes, I do trust explicitly HealthVault issued certificates," not because the federal PKI bridge tells me to trust them, but because I have a relationship with Microsoft HealthVault as an organization. I'm a healthcare provider. I'm Mass General, right? Mass General has a relationship with HealthVault. They are directly trusting HealthVault issued certificates.

So that's a perfectly legitimate policy allowance and the ramification is, again, not much different than the other one and that is the certificate authorities that you trust are the certificate authorities that you trust. Don't trust a certificate authority that you don't trust. I mean it sounds silly, but unfortunately, you have to say it that way or people start to get really relaxed and trust anything.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
If that interoperability with the federal bridge would simplify things, because we have no governance mechanism in place otherwise, to figure out who to trust and who not to trust, but if you kind of default to the federal bridge, if you're cross certified with the federal bridge then we trust you it really simplifies things.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Well, it simplifies, but it doesn't necessarily make life perfectly simple. There are plenty of certificates out there that are perfectly trustable to the federal PKI bridge, but I wouldn't trust the health data that comes out of those organizations for anything.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, yes. That's true. That's true. But at least you—

John Moehrke – Interoperability & Security, GE – Principal Engineer
So—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Nothing we say about these certificates says anything about the data that's being exchanged, that are being exchanged. It says only that the entity is who they claim to be.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Right. So therefore, a reminder and this is a good point to bring the reminder out, that a highly trusted identity does not mean that they should be authorized to do everything possible. So, separate authorization from this authentication step, which is the X.509 certificate and trust.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Good point. It's 12:15 or 3:15 your time. Walter, why don't you walk through the rest of the slides?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. Well, the rest of the slides are really background material, so we don't ... there. We have heard basically and have had a very good and very opaque and broad discussion around the requirements, the criteria ... conceptually what we would need to do next with respect to entity level, digital certificates. I think—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Why don't we go back to slide seven, which has our schedule, just to review what we're going to do on March 9th? I'll write up, before we communicate anything to the Policy Committee, I'll write up these conclusions that we came to and get it to all of you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO

Yes. Okay. So the next step basically is our next call, which is scheduled for March 9th. At that point I think we will bring back, based on all of this discussion, the recommendations regarding digital certificates in terms of this requirement and evaluation and also the communication that would be then brought up to the Policy Committee. So that would be one of part of the call.

Then the second part of the call is really focusing on the provider directory. You should all have received as part of the packet a copy of the recommendations that were presented from the Policy Committee's Information Exchange Workgroup and the Policy Committee to the Standards Committee back in, I think it was, mid-January or late January. We describe basically the elements; I mean the policy recommendations on entity level provider directories, so you should have all received that. That will be the focus of attention of our call then on March 9th. It's really to review the recommendation on entity level provider directory from the Policy Committee and then hear from NW-HIN or NHIN Exchange and the Direct Project how they're approaching entity level provider directories. So that's the focus of our call on March 9th.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So, back to you, Dixie, for any other closing comments.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you very much, Walter. I'll write down these couple of things and distribute it to everybody for your review before we send it off to anybody. Are there any more comments before we open it up to public comments?

Ed Larsen – HITSP
Dixie, just a quick comment for Walter. Kind of buried it in the tier-two was an evaluation of the standards body that was supporting the chosen standard. You've got a number of the kind of points about what's availability and cost, but we also had the preference for a consensus based standards body with a stable business model to be able to support and update their standard.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thank you, Ed. You're saying that that was part of our tier-two back then, right?

Ed Larsen – HITSP
Well, we've kind of separated it out, but it was one of the requirements. It was an evaluation of a preferred standards development organization.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. Good point. We'll add that to the criteria evaluation of the preferred—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Walter, I think it would be worthwhile for you to look at that list of criteria that came out of the things the adoption workgroup, the one that Carol Diamond always cites. It's a list of attributes for adopted standards that we use across all standards from the Standards Committee. I think it would be useful to look at that list and make sure that we've incorporated them in these two tiers as well.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay. I will do that. That was from Carol Diamond, right? Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, yes. It's been presented at our Standards Committee meeting many times.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Judy?

Judy Sparrow – Office of the National Coordinator – Executive Director
Let's ask the public, please, if anybody wishes to make comment, operator. While we're waiting I think I'm going to try to make a call on March 16th if that's okay with Dixie and Walter, some time sort of late morning?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. That's fine with me.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's fine with me too.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. I'll send out an invite to everybody.

Operator
We do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay. Thank you. Thank you, Dixie and Walter.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay. Thank you, all, for dialing in—

(Audio ends abruptly)